Сергей Медведев

Руководитель направления предоставления данных об угрозах
экспертного центра безопасности Positive Technologies

Максим Похлебин

Старший специалист, отдел исследования киберугроз
экспертного центра безопасности Positive Technologies

Мир киберугроз с threat intelligence — задачи, не ограниченные индикаторами компрометации

Задачи Threat Intelligence

Сбор и поставка IOC

Взаимодействие с другими командами

Сбор данных о группировках

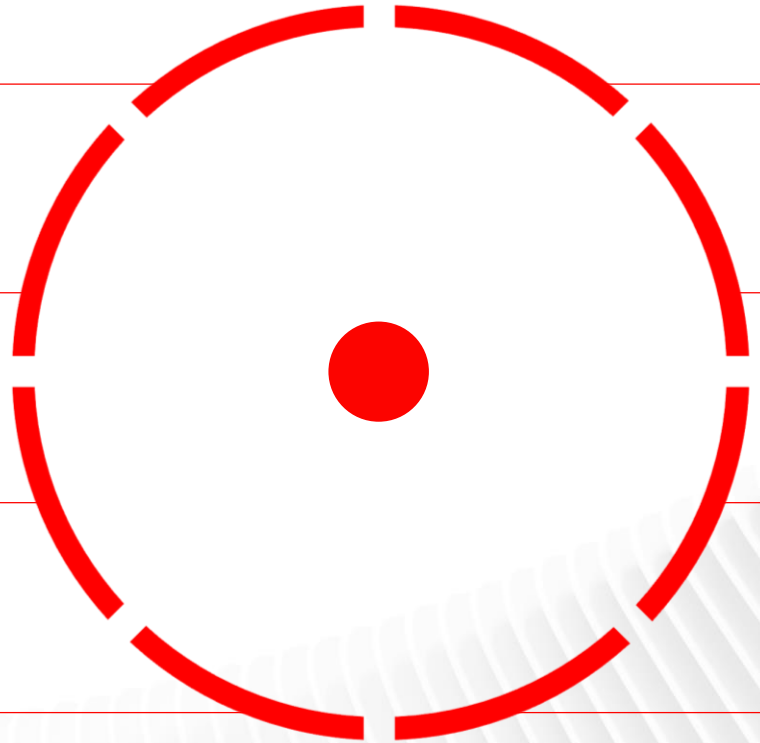
Работа с уязвимостями

Анализ TTP хакерских группировок

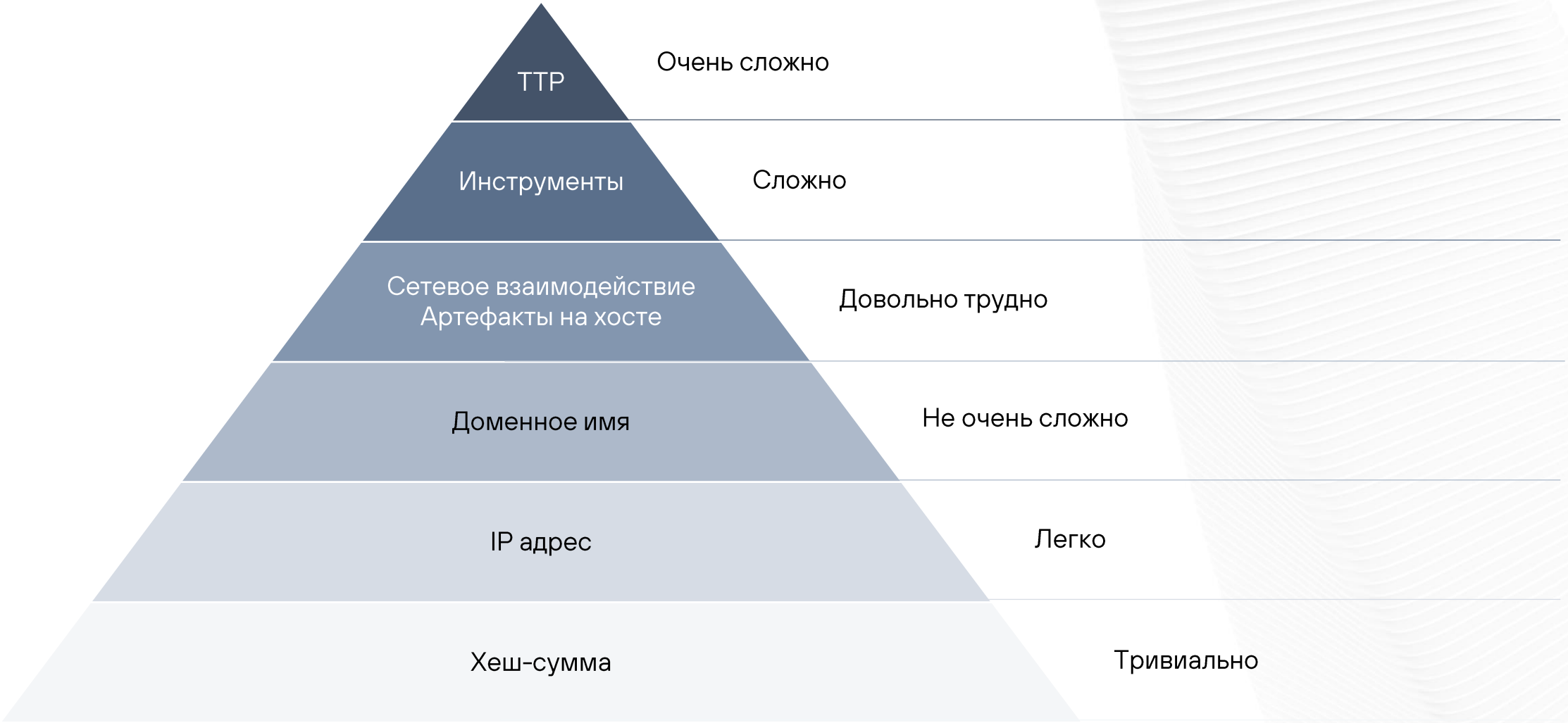
Подготовка отчетов

Анализ ВПО и сетевой инфраструктуры

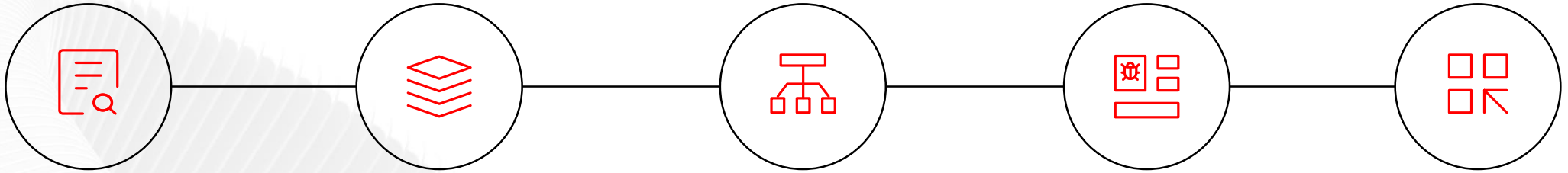
Мониторинг известных и исследование новых угроз



«Пирамида боли»



Анализ ВПО



Статический и динамический анализ

- Сканирование YARA-правилами
- Запуск в песочнице PT Sandbox
- Реверс-инжиниринг

Поиск похожих файлов

- Метаинформация
- Строки
- Участки кода
- Поведение

Анализ сетевой инфраструктуры

- Расширение поверхности исследования атаки
- Поиск контрольных серверов

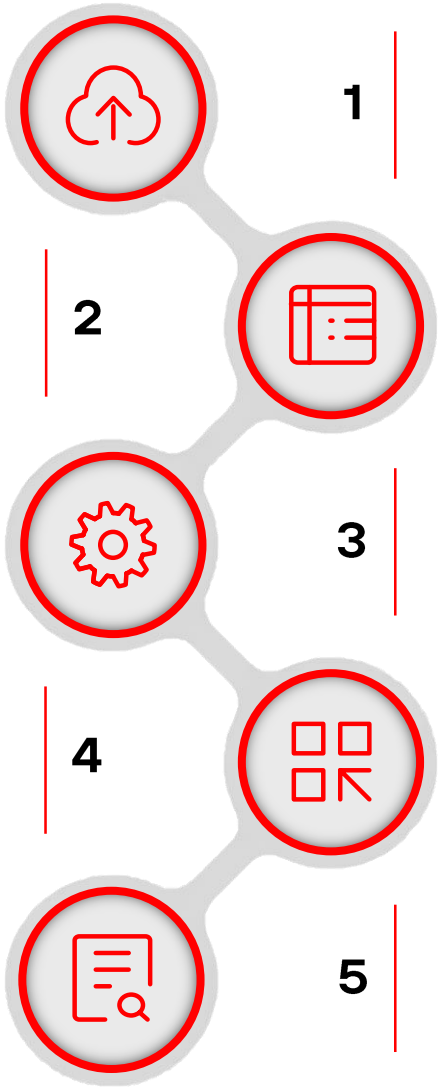
Описание ВПО

- Классификация
- Атрибуция
- Особенности работы
- Индикаторы

Детектирование

- Статическое
- Поведенческое
- Сетевое

ETL-система обработки файлов



1

Источник

Загрузка из различных источников (triage/hybrid/certpl и другие)
Фильтрация
Сохранение в централизованное хранилище
Отправка на обработку

2

Регистратор

Получение истинного формата файла
Получение базовой информации о файле
Отправка на нужный обработчик

3

Обработчик

Извлечение специфичной для формата мета-информации

- исполняемые
- документы
- почта
- архивы
- LNK
- CHM

4

Агрегатор

Объединение полученной информации
Сохранение информации о файле

5

Поиск и просмотр

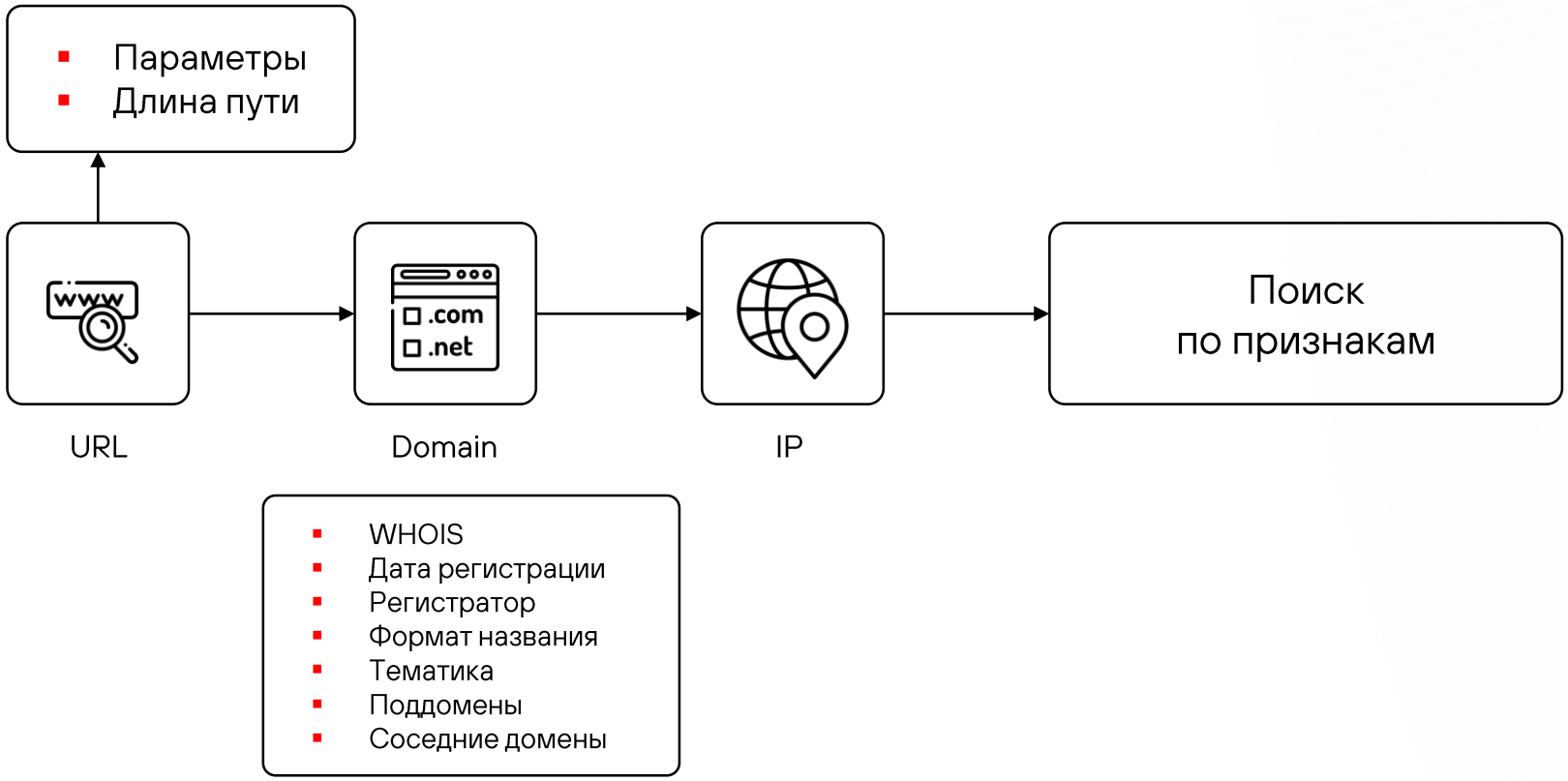
Просмотр информации о файлах
Поиск по полям

Поиск интересных файлов

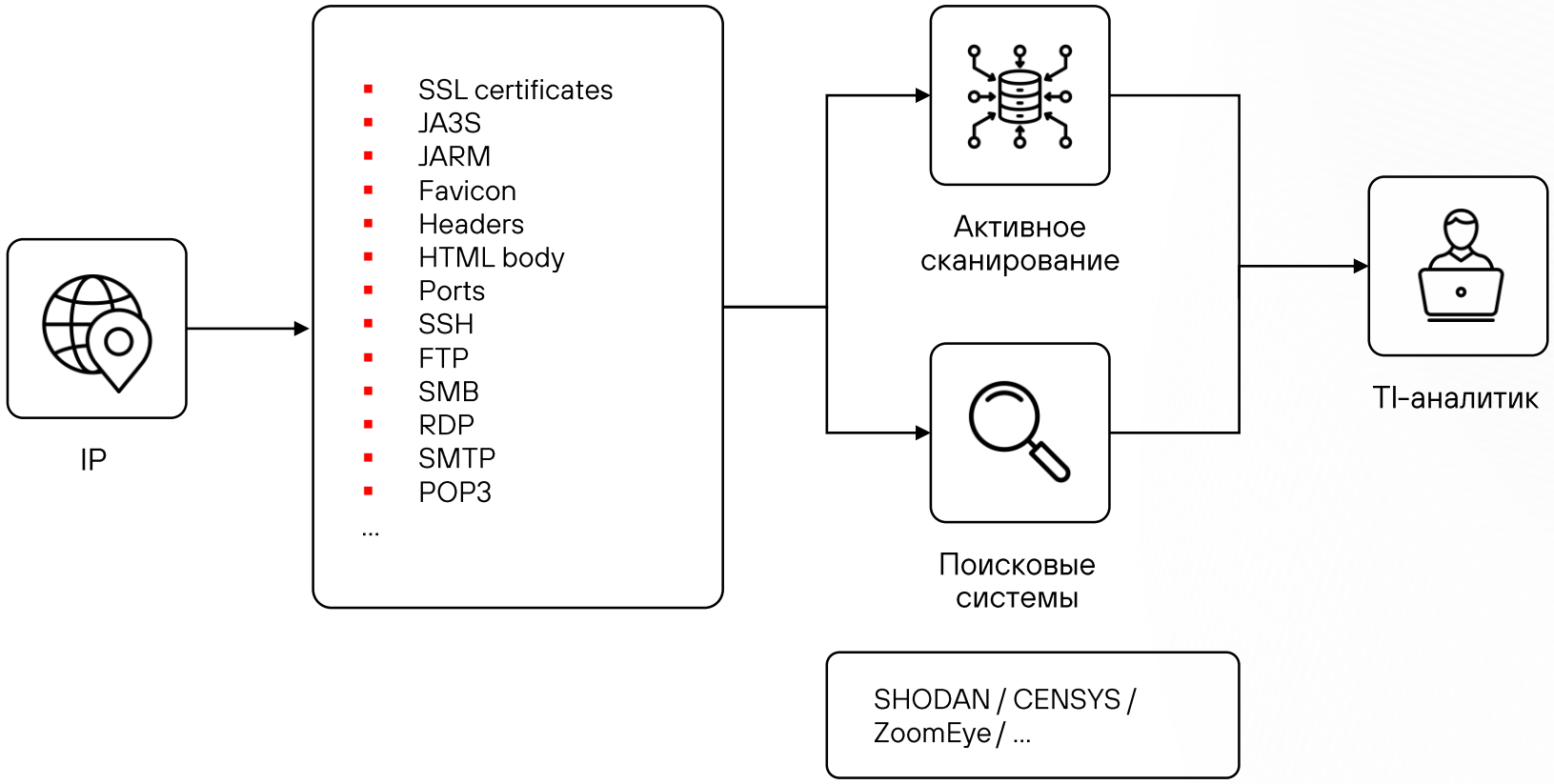
Cloud Atlas

Time	_source
June 2nd 2022, 03:52:01.750	author: pc1q213 threat_actors: tags: yara:OfficeMacro, score:document_with_macros:0.5, from:ptsandbox, macros:run-file, macros:write-file, macros:auto-close, yara:tool, yara:Trojan__Generic__AutoOpen, from:virustotal, score:interesting_country:1.5, yara:ZZ, yara:Risktool__Generic, macros, macros:create-ole, macros:auto-open, yara:win, score:interesting_name:1.5, score:dynamic_malicious:1, from:inquestlab, yara:Trojan__DocumentClose, file:DOC submissions_times: 2 sha256: 256d3065de2345a6beff9458ad0b519bed8363ac0b984247768bd788e633e371 reputation: 50 files_created: contacted_ips: 52.109.32.63, 213.180.204.127 sandbox behaviour verdicts: Write.Registry.Key.Persistence, Trojan-Dropper.MSOffice.Launcher.a, Read.Process.Handle.Enumeration, Create.Win
June 2nd 2022, 03:38:48.185	author: pc1q213 threat_actors: tags: yara:OfficeMacro, score:document_with_macros:0.5, from:ptsandbox, macros:run-file, macros:write-file, macros:auto-close, yara:tool, yara:Trojan__Generic__AutoOpen, from:virustotal, score:interesting_country:1.5, yara:ZZ, yara:Risktool__Generic, macros, macros:create-ole, score:network_malicious:1, macros:auto-open, yara:win, score:dynamic_malicious:1, from:inquestlab, yara:Trojan__DocumentClose, file:DOC submissions_times: 2 sha256: 37e259d6564071807b7b4266ed1dd8bf2059f3e7f438b8487dd0149e5e0487ec reputation: 50 files_created: contacted_ips: 52.109.76.68, 213.180.204.127 sandbox behaviour verdicts: Write.Registry.Key.Persistence, Trojan-Dropper.MSOffice.Launcher.a, Read.Process.Handle.Enumeration, Create.Win
October 21st 2021, 17:29:04.149	author: pc1q213 threat_actors: tags: file:doc, yara:tool, yara:win, yara:ZZ, yara:OfficeMacro, yara:Risktool__Generic, yara:Trojan__Generic__AutoOpen, from:anyrun, anyrun:macros, anyrun:macros-on-open, anyrun:macros-on-close, from:ptsandbox submissions_times: 1 sha256: 62347789bf6a5f81e201c20a79a0d4d7425d408ab69ac205d191c9d9a7f1271d reputation: 50 files_created: contacted_ips: sandbox_behaviour_verdicts: Create.Window.Hidden.Evasion files_written: children: magic: application/msword embedded_filenames: dropped_files: content: crc32: 1,821,564,661 entropy: 6.109 embedded_emails: submitter_country: RU submitter_id: sha512: 0b4e047b0f4f54142c843319196?f164b557fc673864a631c24e859f63053f5ee0300daced1ddf649e73526db0da4b9bc56d205fe3b7

Анализ сетевой инфраструктуры



Поиск по признакам



Пример поиска Cobalt Strike

TLS

Handshake

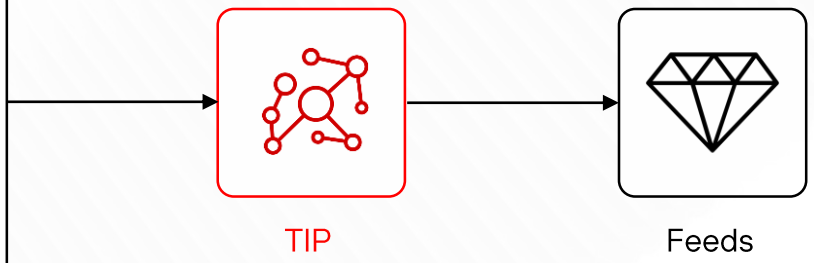
Version Selected	TLSv1_3
Cipher Selected	TLS_AES_256_GCM_SHA384

Certificate

Fingerprint	87f2085c32b6a2cc709b365f55873e207a9caa10bffecf2fd16d3cf9d94d390c
Subject	C=, ST=, L=, O=, OU=, CN=
Issuer	C=, ST=, L=, O=, OU=, CN=

Fingerprint

JARM	2ad2ad16d2ad2ad00042d42d00042ddb04deffa1705e2edc44cae1ed24a4da
JA3S	15af977ce25de452b96affa2addb1036

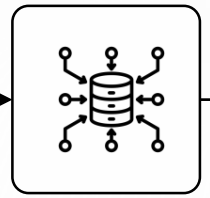


Характерный SSL-сертификат

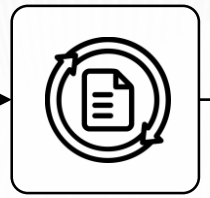
Автоматизация поиска

Алгоритм генерации URL

```
public static long checksum8(String text) {
    if (text.length() < 4) {
        return 0L;
    }
    text = text.replace("/", "");
    long sum = 0L;
    for (int x = 0; x < text.length(); x++) {
        sum += text.charAt(x);
    }

    return sum % 256L;
}

public static boolean isStager(String uri) {
    return (checksum8(uri) == 92L);
}

public static boolean isStagerX64(String uri) {
    return (checksum8(uri) == 93L && uri.matches("/[A-Za-z0-9]{4}"));
}
```

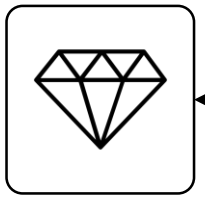


Активное сканирование

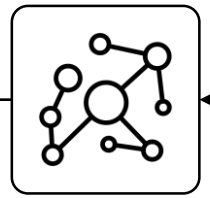


Загрузка и обработка

C2Server	Watermark
https://qw.regcssv.com/fam_calendar, https://as.regcssv.com/fam_calendar, https://zx.regcssv.com/fam_calendar	1580103824
https://Wipro-a7hrgtf0g4ecbtaq.z02.azurefd.net/__utm.gif	1183519219
https://43.153.222.28/updates.rss	100000
https://120.39.197.231/jquery-3.3.1.min.js, https://112.28.231.110/jquery-3.3.1.min.js, https://61.159.80.241/jquery-3.3.1.min.js, https://223.68.136.206/jquery-3.3.1.min.js, https://116.211.153.240/jquery-3.3.1.min.js, https://121.17.123.105/jquery-3.3.1.min.js, https://218.94.206.222/jquery-3.3.1.min.js	391144938
https://service-hlaqy0v7-1303081427.sh.tencentapigw.com/jquery-3.3.1.min.js	100000
https://cdn.microsolt.top/wp-admin, https://cdn.microsolt.top	666666
https://1.15.70.229/s/ref=nb_sb_noss_1/167-3294888-0262949/field-keywords=books, https://www.amazon.com	305419896



Feeds



TIP

Легальные сервисы в качестве C2

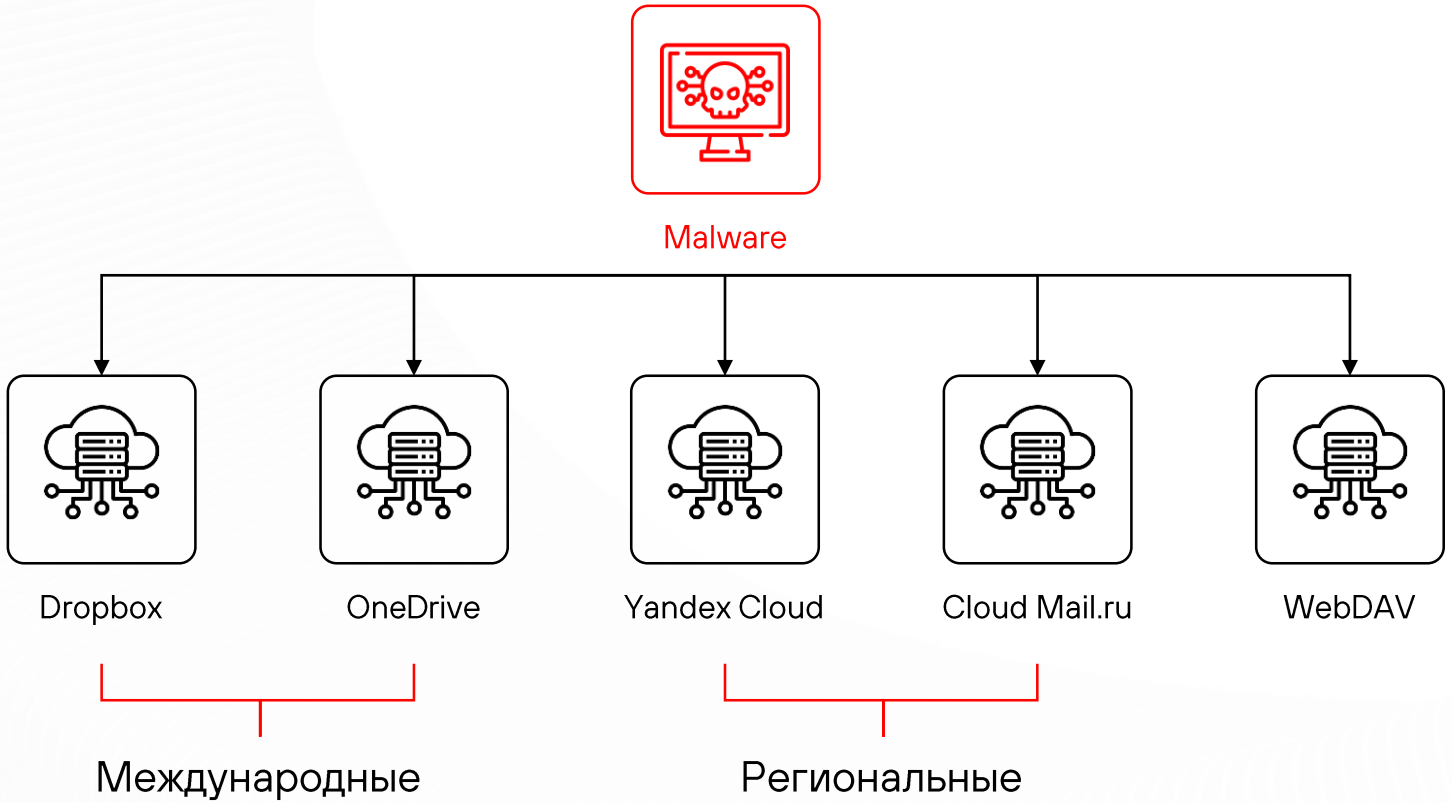
Проблемы:

- Сервисы используются сотрудниками
- Вредоносное взаимодействие похоже на легальный трафик
- Не может быть индикатором компрометации
- Плохо используется для поиска сетевой инфраструктуры хакеров

Решение:

- Исследование API и протокола взаимодействия
- Извлечение полезных данных (паролей, токенов и т.д.)
- Автоматизация извлечения

Cloud C2


Malware
Dropbox
OneDrive
Yandex Cloud
Cloud Mail.ru
WebDAV
Международные
Региональные

Cloud C2. APT31

a.psd

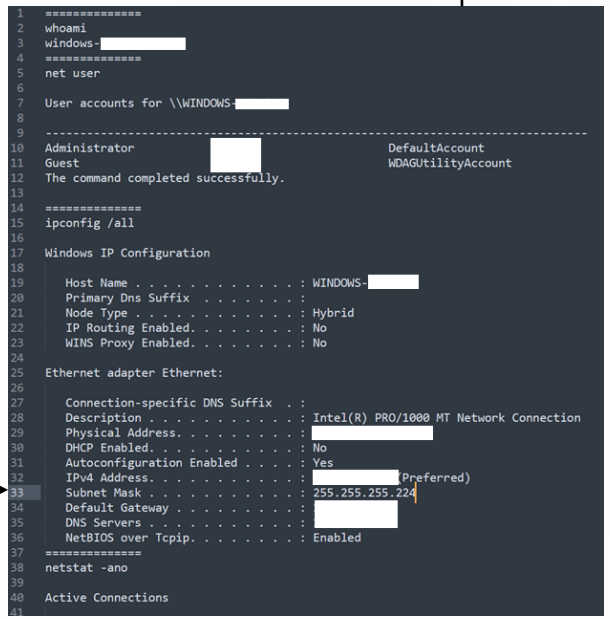
Yandex Disk (https://cloud-api.yandex.net:443/v1/disk/resources?path=[PCNAME])

b.psd

```
1  whoami
2  net user
3  ipconfig /all
4  netstat -ano
5  tasklist
6  systeminfo
7  SLEEP   60
8
```

- DIR
- EXEC
- SLEEP
- UPLOAD
- DOWNLOAD

Malware



Летающие в «облаках»: APT31 вновь использует облачное хранилище, атакуя российские компании
https://www.ptsecurity.com/ru-ru/research/pt-esc-threat-intelligence/apt31-cloud-attacks/

Space Pirates. Voidoor

b0226f19	111.41.144.145	Fri Dec 02, 2022 10:49 am	☐
9d1cca29	111.41.144.145	Fri Dec 02, 2022 10:49 am	☐
435051ee	45.133.181.251	Fri Dec 02, 2022 11:54 am	☐
680588dc	202.182.119.156	Fri Dec 02, 2022 12:27 pm	☐
4b9f65f3	45.133.181.251	Fri Dec 02, 2022 12:28 pm	☐
23777df4	202.182.119.156	Fri Dec 02, 2022 12:37 pm	☐
009d5c98	45.133.181.251	Fri Dec 02, 2022 12:38 pm	☐
bffef065	45.133.181.251	Fri Dec 02, 2022 4:43 pm	☐
b5035046	111.41.144.145	Fri Dec 02, 2022 4:43 pm	☐
b1bcbdd6	111.41.144.145	Fri Dec 02, 2022 4:44 pm	☐
c8411d25	202.182.119.156	Fri Dec 02, 2022 4:45 pm	☐
810392ac	111.41.144.145	Fri Dec 02, 2022 4:46 pm	☐
0b1cef2c	202.182.119.156	Fri Dec 02, 2022 4:59 pm	☐
069f3e16	[redacted]	Fri Dec 02, 2022 5:10 pm	☐
5c6acf0b	202.182.119.156	Fri Dec 02, 2022 5:10 pm	☐
a45ad06e	202.182.119.156	Fri Dec 02, 2022 6:45 pm	☐
2628d653	202.182.119.156	Fri Dec 02, 2022 8:26 pm	☐
68587965	202.182.119.156	Fri Dec 02, 2022 8:30 pm	☐

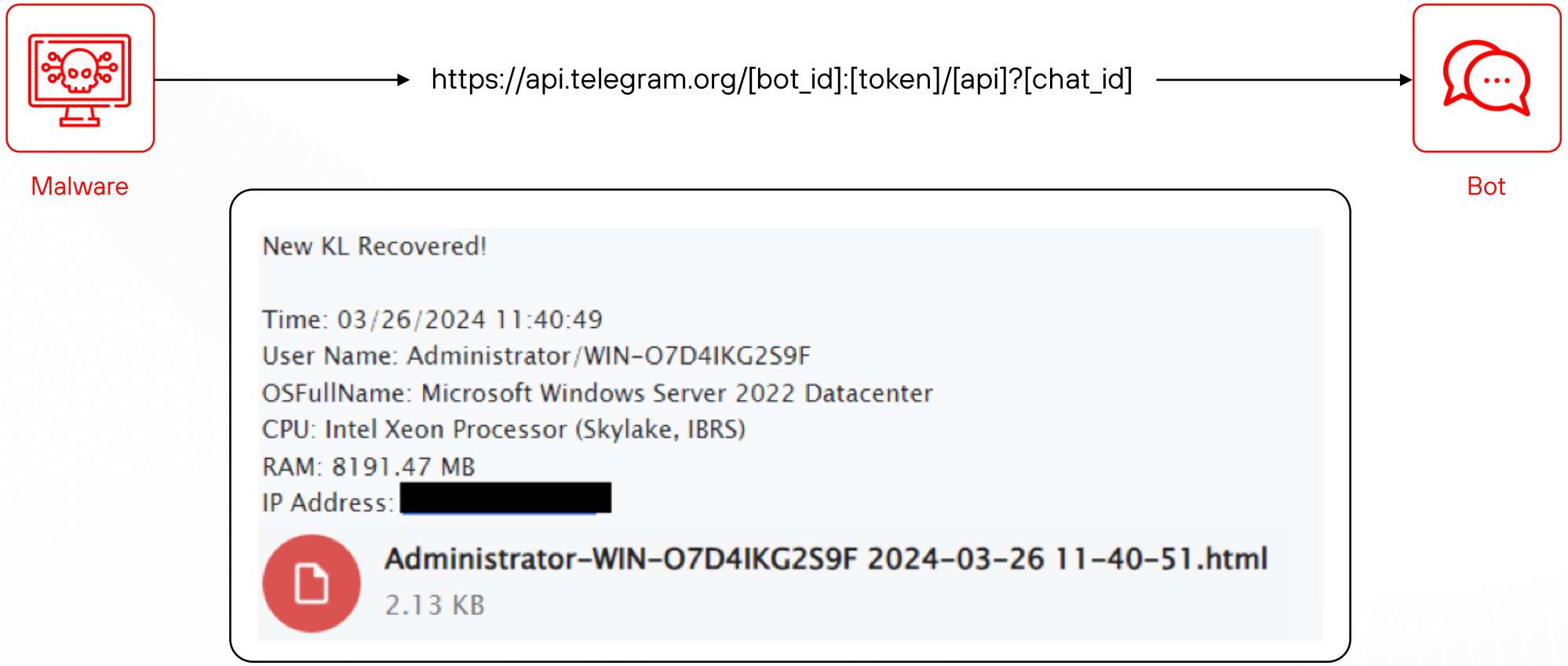
>3500 событий

73 уникальных IP адреса

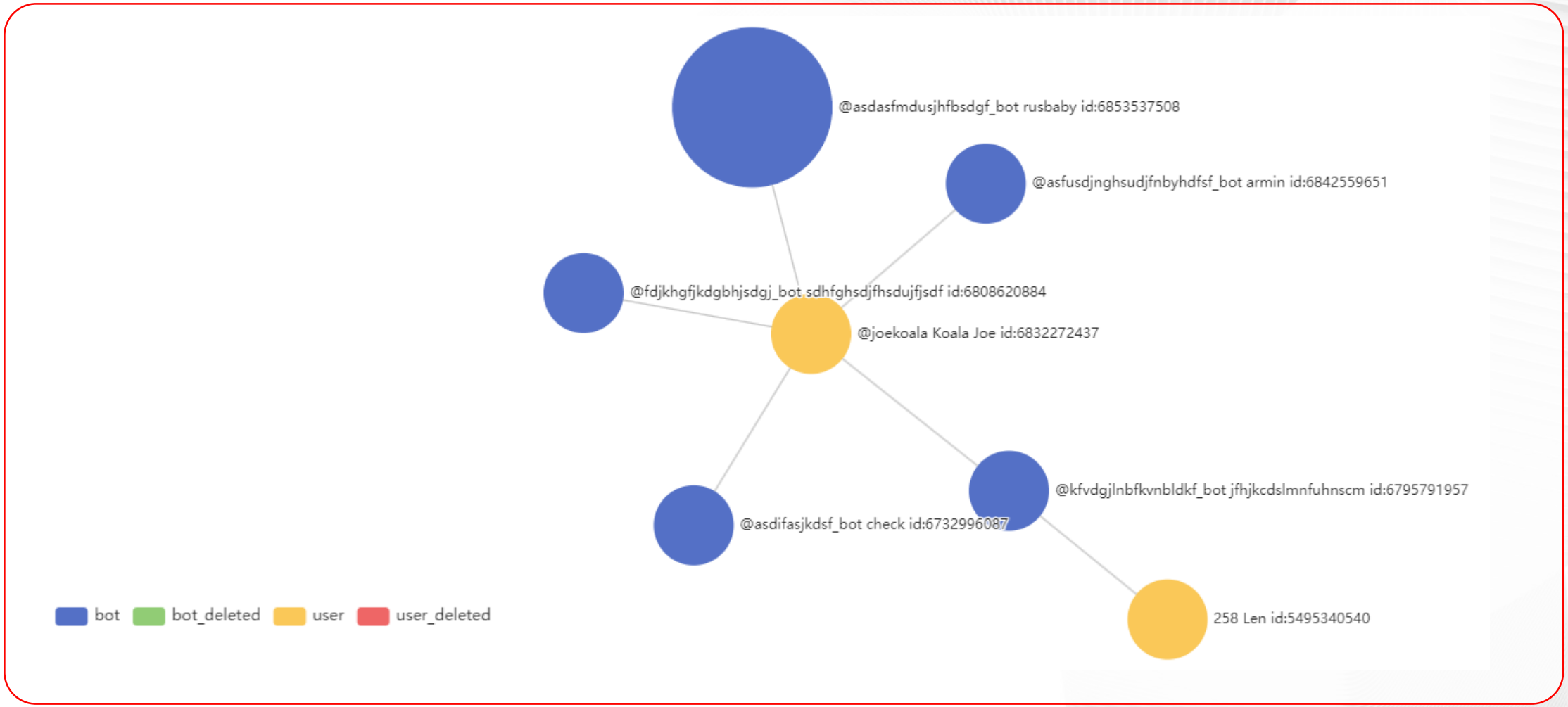
5 C2-серверов Space Pirates

Исследование группировки Space Pirates:
https://www.ptsecurity.com/ru-ru/research/pt-esc-threat-intelligence/space-pirates-exploring-non-standard-techniques-new-attack-vectors-and-grouping-tools/

Telegram


https://api.telegram.org/[bot_id]:[token]/[api]?[chat_id]
Malware
Bot
New KL Recovered!
Time: 03/26/2024 11:40:49
User Name: Administrator/WIN-O7D4IKG2S9F
OSFullName: Microsoft Windows Server 2022 Datacenter
CPU: Intel Xeon Processor (Skylake, IBRS)
RAM: 8191.47 MB
IP Address: [redacted]
Administrator-WIN-O7D4IKG2S9F 2024-03-26 11-40-51.html
2.13 KB

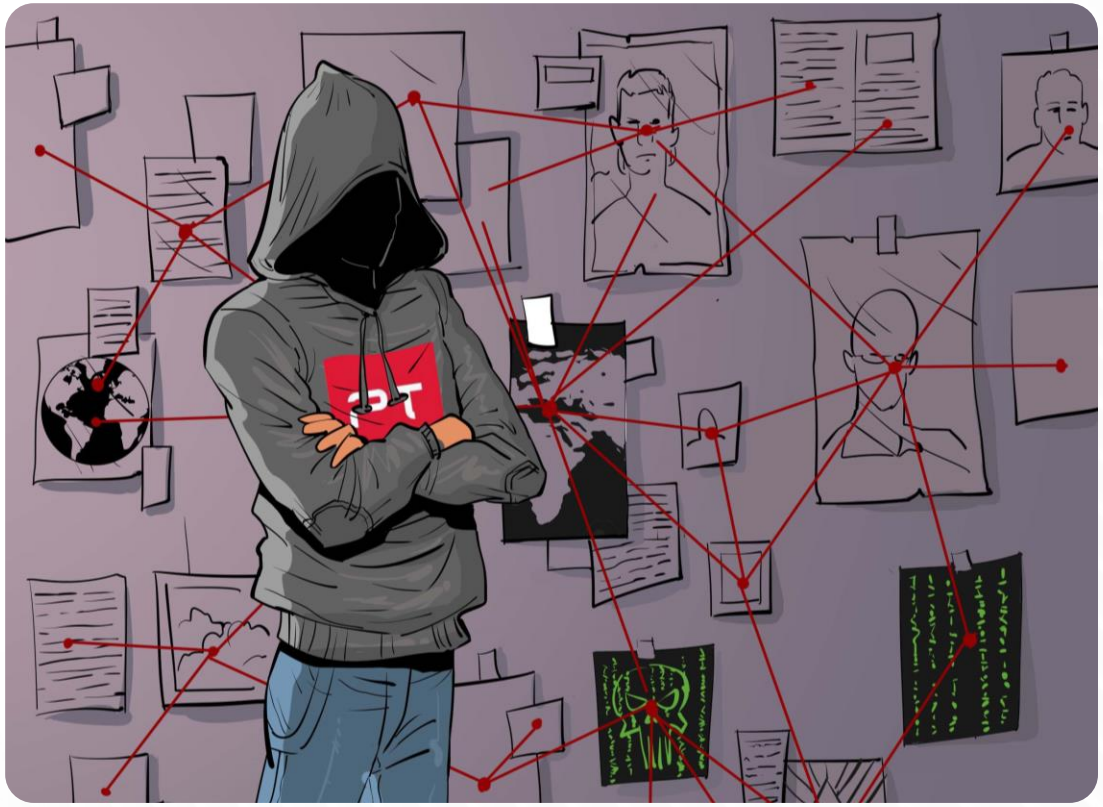
Telegram. Граф связей



LazyStealer: сложно не значит лучше:
https://www.ptsecurity.com/ru-ru/research/pt-esc-threat-intelligence/lazystealer-slozhno-ne-znachit-luchshe/

Поиск взломанных компаний

- Доступ к C2 (использование недостатков)
  - токены доступа
  - артефакты на хосте
  - ошибки в разработке
- Фишинговая рассылка от имени компании, использование ее инфраструктуры в атаке
- Сетевая телеметрия
- Активное сканирование сети Интернет
  - открытые директории
  - поиск бэкдоров
  - потенциальные уязвимости



Ретроспективный анализ группировок

Данные для атрибуции угроз

- Информация, позволяющая устанавливать связь злоумышленника с выявленными угрозами
  - Атрибуция образцов ВПО
  - Атрибуция схемы компьютерной атаки

Оценка покрытия детектирования

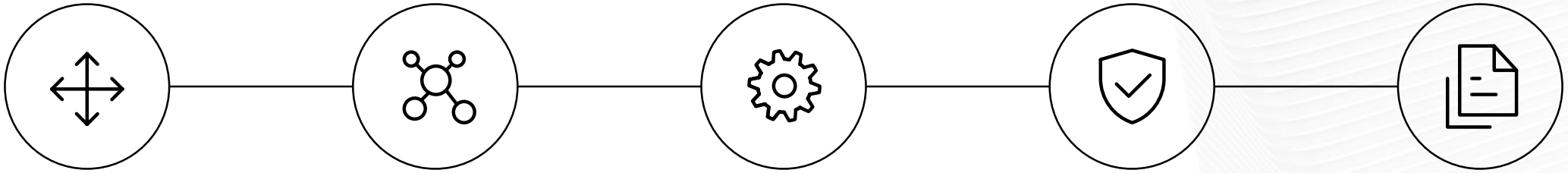
- Проверка фактов детектирования вредоносных техник исследованных образцов ВПО
  - Выявление ошибок
  - Обеспечение детектирования пропущенных техник

Наполнение базы знаний

- Обогащение базы информацией об индикаторах компрометации и наполнение их контекстом

Ретроспективный анализ – это вдумчивое и кропотливое исследование всех имеющих на текущий момент данных о деятельности группировки

Этапы анализа



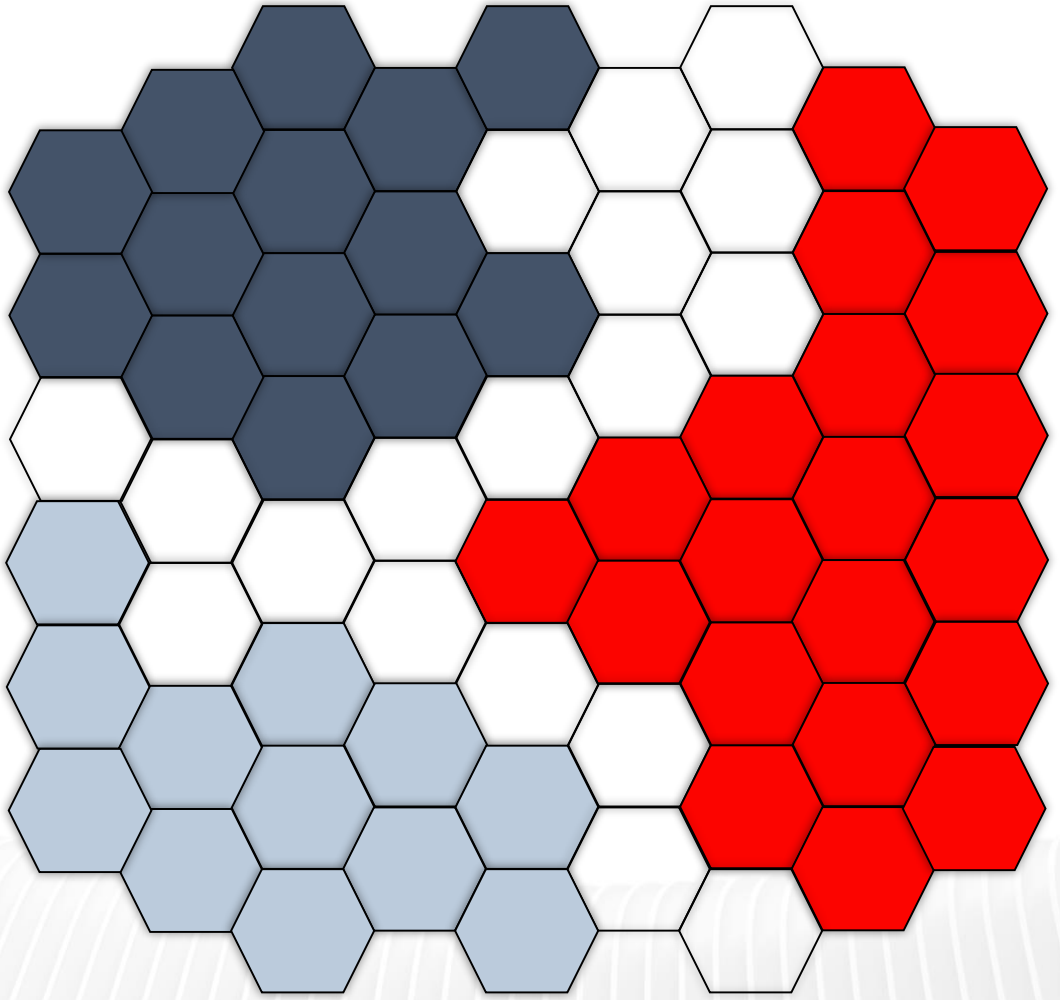
Сбор данных


Детектирующие правила
Общее описание
Таргетинг
Внешние исследования
Векторы атак
СБОР ДАННЫХ
Образцы ВПО
Хакерские инструменты
Хронология активности
Используемые техники
Схемы развертывания

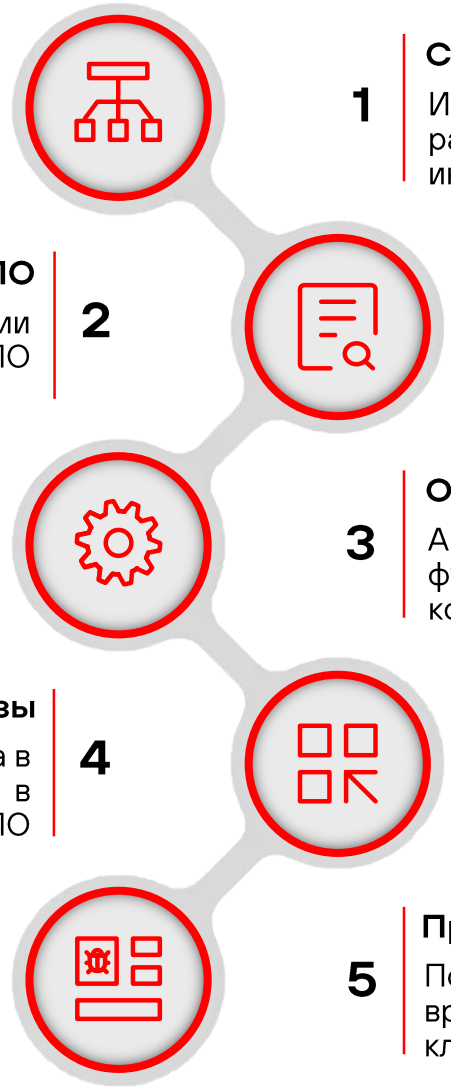
Кластеризация

Собранные данные разделяются по группам для более четкого определения схожих признаков: сначала внутри небольших групп, а потом между группами.

- Кластеризация по хронологии
- Кластеризация по используемым семействам ВПО
- Кластеризация по схемам развертывания ВПО



Анализ кластеров



1 Схемы развертывания

Исследование и описание цепочек развертывания ВПО в атакуемой инфраструктуре

2 Механизмы работы ВПО

Подробное описание реализации вредоносных техник для каждого образца ВПО

3 Особенности функционирования

Аналитика способов атаки и механизмов функционирования ВПО, характерных для конкретных злоумышленников

4 Схожесть кодовой базы

Выявление схожих участков кода в реализациях различных алгоритмов в используемых подсемействах ВПО

5 Профиль вредоносных техник

Построение «тепловых карт» реализации вредоносных техник для анализируемого кластера

Оценка покрытия детектирования

Найденные техники

TA0005 Defense Evasion

- T1055: Process Injection
- T1112: Modify Registry

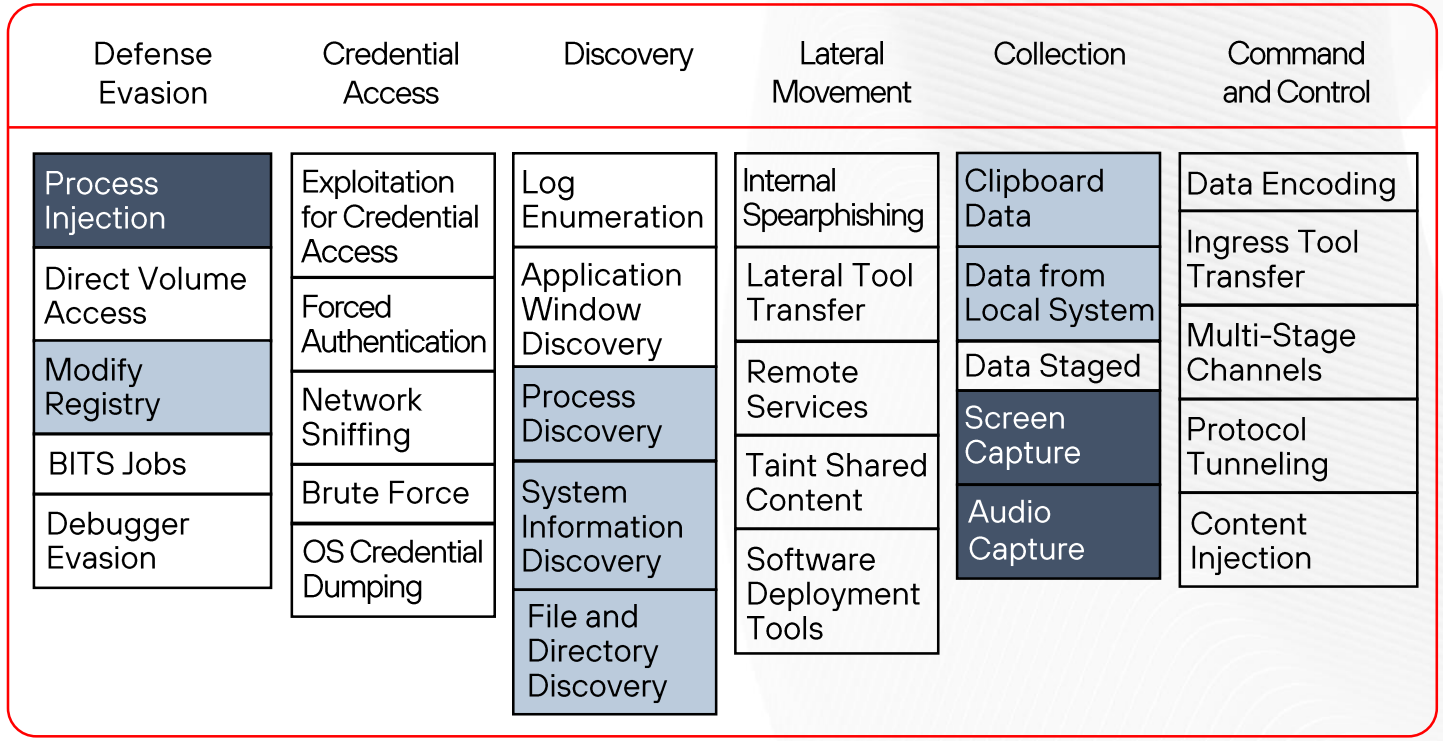
TA0007 Discovery

- T1082: System Information Discovery
- T1083: File and Directory Discovery
- T1057: Process Discovery

TA0009 Collection

- T1005: Data from Local System
- T1115: Clipboard Data
- T1113: Screen Capture
- T1123: Audio Capture

Покрытие детектирования



Подведение итогов

Исследование заканчивается формированием отчетных материалов. Помимо результатов полученных при анализе кластеров, заполняются следующие разделы:

- Общее описание группировки
- Основные отличительные особенности функционирования вредоносных модулей группировки
- Результаты сравнительного анализа образцов между кластерами
- Обобщенная «тепловая карта» используемых техник группировки
- Общий перечень индикаторов компрометации с контекстом

Исследования
PT ESC Threat Intelligence

Исследование о группировке
APT 31

Исследование
о группировке Space Pirates

Исследования
о группировке Lazy Koala

Спасибо!